

S&H Form: PTO/SB/05 (9/99)

# UTILITY **PATENT APPLICATION TRANSMITTAL**

Attorney Docket No. 1614.1085	9 🚍
First Named Inventor or Application Identifier:	
Syuichi SATAKE	6858 6858
Express Mail Label No.	0.00

(Only for	new nonprovisional applications under 37 CFR 1.53(b))	Express Mail Labe	el No.
_/_			3 C
¥	APPLICATION ELEMENTS See MPEP chapter 600 concerning utility patent application contents.	ADDRESS TO:	Assistant Commissioner for Patents Box Patent Application Washington, DC 20231
1. [ <b>X</b> ]	Fee Transmittal Form		
2. <b>[X</b> ]	Specification, Claims & Abstract [Total Pages: 24]		
3. [ <b>X</b> ]	Drawing(s) (35 USC 113) [ Total Sheets: 10 ]		
4. [X]	Oath or Declaration		
5. []	Incorporation by Reference (usable if Box 4b is checked) The entire disclosure of the prior application, from which a considered as being part of the disclosure of the a incorporated by reference therein.	opy of the oath or deaccompanying applic	eclaration is supplied under cation and is hereby
6. [ ]	Microfiche Computer Program (Appendix)		
7. []	Nucleotide and/or Amino Acid Sequence Submission (if appl a. [ ] Computer Readable Copy b. [ ] Paper Copy (identical to computer copy) c. [ ] Statement verifying identity of above copies	licable, all necessar	V)
	ACCOMPANYING AP	PLICATION PAR	RTS
8. [X]	Assignment Papers (cover sheet & document(s))		
9. []		[ ] Power of Attorn	ey
10. [ ]	English Translation Document (if applicable)		
11. [X]	Information Disclosure Statement (IDS)/PTO-1449[X] Copie	s of IDS Citations	
12. [ ]	Preliminary Amendment		
13. [ ]	Return Receipt Postcard (MPEP 503) (Should be specifically	ıtemized)	
14. [ ]	Small Entity Statement(s) [ ] Statement filed in prior app	olication, status still	proper and desired.
15. [X]	Certified Copy of Priority Document(s) (if foreign priority is cla	aimed)	
16. [ ]	Other:		
17. If a	CONTINUING APPLICATION, check appropriate box a	nd supply the requis	site information:
	Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of p		
18. CO	RRESPONDENCE ADDRESS		



PATENT TRADEMARK OFFICE

	Attorney Docket No.	1614.1085	o ==
NEW APPLICATION FEE TRANSMITTAL	Application Number		359 PT
	Filing Date	October 11, 2000	6 U.S
T = 1101 0.0 = 0			00 <b>€</b> 0

				Filing Date		October 11, 2000			/685 /11/	
AMOUNT ENC	LOSED	\$	970.00	First Na	med Inventor	Syu	ıichi SAT	AKE		000 En
FEE CALCULATION (fees effective 10/01/97)										
CLAIMS	(*	(1) FOR (2) NUMBER FILED (3) NUMBER EXTRA (4) RATE			(5) CA	(5) CALCULATIONS				
	TOTAL CI	LAIMS	12	- 20 =	0		X \$ 18.0	0 =	\$	0.00
	INDEPEN	DENT CLAIMS	6	- 3 =	3		X \$ 80.0	0 =		240.00
	MULTIPLI	E DEPENDENT C	CLAIMS (any i	number; if a	oplicable)		+ \$240.00	0 =		0.00
					ВА	SIC	FILING F	EE		710.00
					Total	of abo	ve Calcula	tions =	\$	930.00
	Surcharge	for late filing fee,	Statement or	Power of A	ttorney (\$130.00)				+	0.00
	Reduction	by 50% for filing	by small entit	y (37 CFR 1	.9, 1.27 & 1.28).					0.00
			<u> </u>		TOT	TAL F	ILING F	EE =	\$	930.00
Surcharge for filing non-English language application (\$130.00; 37 CFR 1.52(d))				+	0.00					
	Recordation of Assignment (\$40.00; 37 CFR 1.21(h)(1))				+	40.00				
					TC	TAL	FEES D	UE =	\$	970.00
	·		METH	OD OF I	PAYMENT			·-···		
	closed as	•								
		ES DUE" to the	•		•	سمطفر	:	.:. 4:		
[] No payin	ent is entir				it Account are a	utnor	ized at tr	iis time	),	
			CLOSED" i	s not corr	ect, the Commis	ssione	er is here	eby aut	horized	d to credit an
De	Deposit Account No. 19-3935									
Deposit Account Name STAAS & HALSEY LLP										
[X] The Commissioner is also authorized to credit any overpayments or charge any additional fees required under 37 CFR 1.16 (filing fees) or 37 CFR 1.17 (processing fees) during the prosecution of this application, including any related application(s) claiming benefit hereof pursuant to 35 USC § 120 (e.g., continuations/divisionals/CIPs under 37 CFR 1.53(b) and/or continuations/divisionals/CPAs under 37 CFR 1.53(d)) to maintain pendency hereof or of any such related application.										
SUBMITTED BY: STAAS & HALSEY LLP										
Typed Name	H. J. Staa	as				Re	eg. No.	22,01	0	
Signature		M	Rav				ate		oer 11,	2000

© 1997, 1998 Staas & Halsey LLP

#### SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT I, Syuichi Satake, a citizen of Japan residing at Nei, Japan have invented certain new and useful improvements in

APPARATUS AND METHOD FOR AUTHENTICATING
DIGITAL SIGNATURES AND COMPUTER-READABLE
RECORDING MEDIUM THEREOF

of which the following is a specification : -

#### TITLE OF THE INVENTION

APPARATUS AND METHOD FOR AUTHENTICATING DIGITAL SIGNATURES AND COMPUTER-READABLE RECORDING MEDIUM THEREOF

5

10

15

20

25

30

35

# BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to apparatuses and methods for authenticating digital signatures and computer-readable recording media having a program recorded therein for causing a computer to authenticate a digital signature, and more particularly to an apparatus and a method for authenticating a digital signature, and a computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, in which apparatus, method and medium the digital signature is formed by a random unintelligible number or character string and a signature mark of a signer can be built into image information so that the digital signature can be visually recognized.

2. Description of the Related Art
In a network such as a client/server
system shown in Fig.1, a plurality of clients and a
server are connected through the network. In such a
network system, an electronic decision system is
widely known in which a decision transaction is
conducted by utilizing GroupWare.

In the electronic decision system, a digital signature is used. For example, in Fig.1, a user A of a client A attaches a digital signature to a document created by the user A and then sends the document to a user B of a client B through the network. The user B of the client B obtains a public key for decrypting the digital signature of the user A of the client A and decrypts the digital signature

15

20

25

30

attached to the document received from the user A by using the public key. When the digital signature is successfully decrypted, the document is authenticated so as to be sure that the document was sent from the user A and was not tampered with. As described above, it is possible to authenticate a document author (document sender) by using the digital signature. Thus, it is not required for the document author to print out a created electronic document onto a paper sheet and then stamp a personal seal on this paper sheet where the created electronic document was printed.

However, the conventional digital signature described above has disadvantages.

Generally, the digital signature is formed by a random unintelligible number or character string. Thus, the digital signature can not be recognized easily by human eyes while a stamped seal identifying the document author can be easily recognized by human eyes. Accordingly, it is difficult for a receiver which has received the created electronic document from the document author to distinguish a difference between a legal digital signature and an illegal digital signature of the document author. Also, the digital signature formed by an unintelligible number or character string makes the receiver uncomfortable and it is required for the receiver to decrypt the digital signature.

Moreover, the digital signature recently has become 512 to 1024 bits in length. Compared with the seal stamped on the paper sheet, a larger space is required to show the digital signature.

Also, the digital signature conventionally has another disadvantage in that a position of the digital signature is limited to an end of the created document, while there is no limitation on where to stamp a seal on the paper sheet.

#### SUMMARY OF THE INVENTION

5

10

15

20

25

30

It is a general object of the present invention to provide an apparatus for authenticating a digital signature in which the above-mentioned problems are eliminated.

A more specific object of the present invention is to provide an apparatus and a method for authenticating a digital signature, and a computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, in which apparatus, method and medium the digital signature is formed by a random unintelligible number or character string and a signature mark of a signer can be built into image information so that the digital signature can be visually recognized.

The above objects of the present invention are achieved by an apparatus for authenticating a digital signature, including: a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature; a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and an image embedding part embedding the image information created by the signature synthesizing part into an indicated position in the digital document.

According to the present invention, the digital signature is created by encrypting the private key for authenticating the signer and the digest key for validating the digital document.

Further, the digital signature is built in the image information and then the image information including the digital signature is embedded in the digital

15

20

35

document. Therefore, it is possible for a receiver receiving the digital document including the digital signature through the network to visually distinguish that the mark represented by the image information is sent form the signer. In addition, it is possible for the receiver to simultaneously authenticating the signer and validating the digital document.

The above objects of the present invention are achieved by an apparatus for authenticating a digital signature, including: a signature extracting part extracting the digital signature from image information embedded into a digital document; a digest obtaining part decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and an authenticating part determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by the digest obtaining part and authenticating the digital signature based on a result of the determination.

According to the present invention, the digital signature is authenticated by comparing the first digest information obtained by decryption with the second digest information regenerated from the digital document. Therefore, as a result of comparison, when the first digest information identically corresponds to the second digest information, the signer is authenticated and the digital document is validated at the same time.

Moreover, the above objects of the present invention are achieved by a method for authenticating a digital signature, including the steps of: (a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been

10

30

35

tampered with, and generating a digital signature; (b) creating image information by synthesizing the digital signature and a predetermined mark; and (c) embedding the image information created in the step (b) into an indicated position in the digital document.

According to the present invention, it is possible to provide the method for authenticating a digital signature in which method the digital signature, which is generated from a random number or character string, can be imaged to be visually recognizable.

The above objects of the present invention are also achieved by a method for authenticating a digital signature, including the steps of: (a) 15 extracting the digital signature from image information embedded into a digital document; (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document 20 has been tampered with; and (c) determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by the step (b) and authenticating the digital signature based on a 25 result of the determination.

According to the present invention, it is possible to provide the method for authenticating a digital signature in which method the signer can be authenticated and the digital document can be validated simultaneously.

Furthermore, the above objects of the present invention are achieved by a computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, including the codes of: (a) encrypting a digital document by using a private key defined by a

10

signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature; (b) creating image information by synthesizing the digital signature and a predetermined mark; and (c) embedding the image information created in the step (b) into an indicated position in the digital document.

According to the present invention, it can be realized by a computer installing the codes from the computer-readable recording medium that the digital signature, which is generated from a random number or character string, can be imaged to be visually recognize.

The above objects of the present invention are achieved by a computer-readable recording medium 15 having a program recorded therein for causing a computer to authenticate a digital signature, including the codes of: (a) extracting the digital signature from image information embedded into a digital document; (b) decrypting the digital 20 signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and (c) determining whether second digest information regenerated based on the digital document identically 25 corresponds to the first digest information obtained by the code (b) and authenticating the digital signature based on a result of the determination.

According to the present invention, it can be realized by a computer installing the codes from the computer-readable recording medium that the signer can be authenticated and the digital document can be validated simultaneously.

#### 35 BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features and advantages of the present invention will become more apparent from

20

the following detailed description when read in conjunction with the accompanying drawings, in which:

FIG.1 is a diagram illustrating a
client/server system;

FIG.2 is a block diagram of a hardware configuration of an apparatus for authenticating a digital signature according to an embodiment of the present invention;

FIG.3 is a flowchart for explaining a 10 registration process for seal information;

FIG.4A is a diagram illustrating a setting window for seal-image personal information and FIG.4B is a diagram illustrating a registration window of a seal image;

FIG.5 is a flowchart for explaining a process for embedding the seal image into a document;

FIG.6A is a diagram illustrating an execution window for stamping a seal on an opened document and FIG.6B is a diagram illustrating a confirmation of the stamped seal onto the opened document;

FIG.7 is a flowchart for explaining processes for authenticating the digital signature;

FIG.8A is a diagram illustrating an authentication window for authenticating a stamped seal image and FIG.8B is a diagram illustrating an authentication result window when the stamped seal image is successfully authenticated;

FIG.9 is a diagram illustrating another authentication result window when the stamped seal image is not authenticated; and

FIGS.10A, 10B and 10C are diagrams for explaining a process for decrypting the seal image.

## 35 DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG.2 is a block diagram of a hardware configuration of an apparatus for authenticating a

35

digital signature according to an embodiment of the present invention.

In FIG.2, the apparatus as a computer system includes a CPU (Central Processing Unit) 11, a memory unit 12, an input unit 14, a display unit 15, a storage unit 16, a CD-ROM driver 17 and a communication unit 18, which are mutually connected by a bus B.

system in accordance with a program resident in the memory unit 12. In addition, the CPU 11 executes processes for authenticating a digital signature that will be described later. The memory unit 12 includes ROM and RAM. Also, the memory unit 12 temporarily stores programs and various data necessary for or obtained from executions of the processes. In addition, a part of the memory unit 12 is assigned as a working area accessed by CPU 11.

The input unit 14 includes a keyboard and a mouse but is not limited to only these input devices. The input unit 14 is used for a user to register and change information for an authentication process, and to input information into the computer system. The display unit 15 displays results of various processes or data necessary for the user.

The storage unit 16 includes a hard disk and stores various data and programs.

In accordance with instructions from the CPU 11, the CD-ROM driver 17 reads information from the CD-ROM 20 set in the CD-ROM driver 17 and then provides the information to the storage unit 16. For example, various programs according to the present invention are provided by the CD-ROM 20. That is, the programs read from the CD-ROM 20 are installed in the storage unit 16 through the CD-ROM driver 17. It should be noted that a recording medium is not limited to the CD-ROM 20, but another computer-

readable recording medium such as a magnetic disk, a magnetic tape, an optical disk, a magneto-optical disk, a semiconductor memory or the like may be used.

A registration process for seal

information will be described with reference to FIG.3,
FIGS.4A and 4B, according to the embodiment of the
present information. FIG.3 is a flowchart for
explaining the registration process for the seal
information. FIG.4A is a diagram illustrating a

setting window for seal-image personal information.
FIG.4B is a diagram illustrating a registration
window of a seal image.

In FIG.3, a user A using a client A opens a setting window 41 shown in FIG.4A at the display unit 15 in FIG.2 in order to register seal-image 15 personal information including secret information (a password or the like) and open information (a user name, a job title or the like). Then, in order to register necessary information, the user A inputs an employee number (step S1) and subsequently inputs a 20 seal name (for example, "date seal 1", "private seal 1" or the like) (step S2). When the user A clicks "REGISTRATER", the registration window 43 for a seal image shown in FIG.4B is displayed. At the 25 registration window 43, the user A inputs a name (step S3) and a job title (step S4). Furthermore, the user A selects one seal shape (step S5) and then indicates a seal size, for example, in millimeters (mm) (step S6). For illustration, the user A registers "FUJI" for the name, "DEVELOPMENT SECTION 30 MANAGER" for the job title, "ROUND (DATE REQUIRED)" for the seal shape, and "12" mm for the seal size. In this case, a seal image is generated based on the above input information and a seal image display area 45 shows the seal image (step S7). The user A 35 registers the seal image by clicking "REGISTRATER". The above input information and the seal image

10

20

25

30

generated in the step S7 are registered in the storage unit 16 in FIG.2. When the user A wishes to cancel registering the input information or the seal image, the user A clicks "CANCEL".

The seal image may also be registered in the storage unit 16 after being scanned by a scanner. That is, an electronic signature generated when a signature handwritten by the user A is scanned can be registered in the storage unit 16 as a private seal image. When the seal image is drawing (vector) information, it is not required to scan the seal image.

As described above, the storage unit 16 in FIG.2 stores the open information (the employee number, the name, the job title or the like for the user A), and the seal name and seal image information including the seal shape and seal size) registered by the user A from the setting window 41 in FIG.4A and the registration window 43 in FIG.4B.

The user A creates a document and embeds the registered seal image into the document.

A process for embedding the seal image into the document will now be described with reference to FIG.5, FIG.6A and FIG.6B. FIG.5 is a flowchart for explaining the process for embedding the seal image into the document. FIG.6A is a diagram illustrating an execution window for stamping a seal on an opened document and FIG.6B is a diagram illustrating a confirmation of the stamped seal onto the opened document.

In FIG.5, the user A opens the execution window 61 in FIG.6A on the document created by the user A and indicates an area 63 for embedding the seal image registered beforehand (step S11).

35 Subsequently, the user A inputs the employee number, for example "1234567890", the seal name and a private key into respective predetermined input fields, and

25

30

then clicks "STAMP" on the execution window 61 (step S12). By clicking "STAMP", the CPU 11 in FIG.2 of the client A used by the user A generates an MD (message digest) file (or digest information)

5 ensuring contents of the document created by the user A (sealed document) (step S13). Subsequently, the CPU 11 encrypts the digest information generated in the step S13 (step S14). Accordingly, the digital signature, which is formed by an unintelligible number or character string, is created by encrypting the digest information in accordance with a predetermined method based on the private key defined by the user A.

The CPU 11 searches the storage unit 16 in FIG.2 for seal image data registered by the user A based on the employee number and the seal name indicated by the user A on the execution window 61.

The CPU 11 regenerates the seal image from the seal image obtained from the storage unit 16 (step S15). The digital signature created from the digest information is embedded into the seal image regenerated in the step S15 (step S16). In detail, a process for building the digital signature into the seal image will be described later. The seal image the built-in digital signature is embedded into the area 63 of the document, which was indicated by the user A when the execution window 61 was opened. Then the seal image is displayed as an embedded seal image in an embedded area 67 of the document in FIG.6B and the confirmation window 65 shown in FIG.6B is displayed on the document (step S17). When the user A clicks "OK", it is confirmed that the seal image is to be embedded into the document. The process is then completed.

Accordingly, the digital signature can be embedded with the seal image into the document such as an HTML (Hyper Text Markup Language), an SGML

25

30

35

(Standard Generalized Markup Language), an XML (eXtensible Markup Language) or the like and can be sent to a client B through the network.

A process for authenticating a digital 5 signature will now be described in a case in which a document has embedded therein a seal image with the digital signature built in, with reference to FIG.7, FIGS.8A and 8B, and FIG.9. FIG.7 is a flowchart for explaining processes for authenticating the digital signature. FIG.8A is a diagram illustrating an 10 authentication window for authenticating a stamped seal image and FIG.8B is a diagram illustrating an authentication result window when the stamped seal image is successfully authenticated. And FIG.9 is a diagram illustrating another authentication result 15 window when the stamped seal image is not authenticated.

It should be noted that the client B as a receiver implements the hardware configuration shown in FIG.2.

In FIG.7, a user B at the client B indicates a seal area 83 for authenticating the digital signature on a document received from the client A on the display unit 15 in FIG.2 and then the authentication window 81 in FIG.8A is opened (step S41). Subsequently, the user B obtains a public key (step S42). That is, the user B may obtain the public key from a public key list provided by a server on the Internet. In this case, the public key can be searched for by sender name, the employee number of the sender, or other information specifying the sender. The user B inputs the public key obtained in the step S42 into a predetermined input field on the authentication window 81 in FIG.8A and clicks "AUTHENTICATE".

The CPU 11 of the client B extracts the digital signature from the seal image data of the

15

20

25

30

35

seal area 83 and obtains the digital signature, that is, the random number or character string (step S43).

The CPU 11 decrypts the digital signature by the public key obtained in the step S42. Since the digital signature was encrypted by digest information and the private key of the user A, the digest information is extracted after the digital signature is decrypted (step S44). Hereinafter, the digest information may be referred to as decrypted digest information.

Furthermore, the CPU 11 regenerates an MD file (regenerated digest information) of the document received from the user A (step S45). Subsequently, the CPU 11 compares the decrypted digest information extracted by decrypting the digital signature in the step S44 with the regenerated digest information regenerated in the step S45 (step S46) and notifies the user B of a comparison result as an authentication result by displaying the authentication result window 85 (step S47). When the regenerated digest information identically corresponds to the decrypted digest information, the authentication result window 85 shown in FIG.8B is displayed at the display unit 15 in FIG.2 so as to notify the user B that the seal image stamped on the document received from the user A is valid. the legal digest information is obtained in the step S44 and then the user A as a writer is authenticated and it is verified that the document received from the user A has not been tampered with. On the other hand, when the regenerated digest information does not identically correspond to the decrypted digest information, another authentication result window 91 shown in FIG.9 is displayed at the display unit 15 so as to notify the user B that the seal image stamped on the document received from the user A is invalid. That is, the user A as a writer is invalid or the

10

document received from the user A has been tampered with, or both the user A and the document are invalid.

The process for building the digital signature into the seal image will be now described in details with reference to FIGS.10A, 10B and 10C.

Referring to FIG.5, the CPU 11 of the client A at the sender side obtains the private key input by the user A on the execution window 61 shown in FIG.6A (step S12). The CPU 11 generates the digital signature shown in FIG.10A by encrypting the digest information generated in the step S13 by an encryption function. For the sake of convenience, a hex number is used in FIG.10A.

Subsequently, the CPU 11 obtains the seal image generated in the step S15. The seal image is 15 formed by pixel data (bitmap data) and each pixel data is an index number indicating a palette position. In the embedded area 67 of the document that is confirmed on the confirmation window 65 shown in FIG.6B, for example, a background color is white and 20 a seal color (character color) is black. In this case, the pixel data of the seal image obtained is formed by a plurality of index numbers indicating white or black. The CPU 11 replaces the index 25 numbers indicating colors other than the character color (white) with data (hex numbers) of the digital signature from a beginning of the pixel data. example, when the seal image is created, the character color of the seal image is always defined 30 at a beginning of the palette. Since the index number of black is "00 (hex)", the CPU 11 replaces the index numbers with the data of the digital signature while skipping "00 (hex)" in the data of the digital signature. In a header part (not shown) of the seal image including the pixel data, 35 information indicating data lengths of the seal image and the digital signature is additionally provided.

35

The CPU 11 may set color data (for example, RGB data) indicating white to palette positions other than a palette position for black since the palette positions for 256 colors are indicated by the index numbers "00 (hex)" through "FF (hex)". In this case, the CPU 11 sets white color data to palette positions indicated by the index numbers "01 (hex)" through "FF (hex)" other than the palette position for black as the character color indicated by the index number "00 (hex)". Accordingly, as shown in FIG.10C, a palette 10 is created such that the character color is black and background color is white. Thus, the digital signature, which is encrypted and becomes an unintelligible long string, can be built into the 15 seal image so that the user B does not have to be bothered by the unintelligible long string. Also, it is not required to transform the seal image so that the user B can easily distinguish the seal image of the user A by sight.

As described above, the document, which has been embedded therein the seal image having the built-in digital signature is sent to the user B. A process for decrypting the seal image received from the user A will now be described with reference to FIG.10A and FIG.10B.

Referring to FIG.7, in the client B as a receiver, the seal image is extracted by indicating the seal area 83 in FIG.8A on the document received from the user A (the step S41). The pixel data (bitmap data) forming the seal image is shown in FIG.10B. The CPU 11 of the client B obtains the information including the data lengths of the seal image and the digital signature from the header of the seal image. In this case, since the character color is indicated by the index number "00 (hex)", the CPU 11 reads the pixel data from the beginning of the seal image while skipping "00 (hex)" in the pixel

30

data. Then, the CPU 11 extracts the digital signature shown in FIG.10A (the step S43).

Subsequently, the CPU 11 decrypts the digital signature extracted in the step S43 by using the public key obtained in the step S42 and a function such as a decryption function. Then, the digest information is obtained (the step S44).

In the embodiment, the user B obtains the public key from a server providing the public key

10 list. Alternatively, the client A as a sender may set information including the name and the employee number of the user A in the header of the seal image so that the client B as a receiver can obtain the public key from the server. Thus, it is not required for the user B using the client B to access the server to obtain the public key.

Moreover, in the embodiment, the digital signature is built in the background of the seal image. Alternatively, in FIG.10C, instead of "black" indicated by the index number "00 (hex)", "white" can be applied as the character color and instead of "white" indicated by the index numbers "01 (hex)" through "FF (hex)", "black" can be applied as the background color.

According to the present invention, the digital signature is built into an image so as to be imaged. That is, the imaged digital signature, which is generated from a random number or character string, can be visually recognized easily.

In addition, it is possible to reduce an area for displaying the digital signature formed by an unintelligible string having a length of 512 to 1024 bits.

Furthermore, by a combination of the MD file (digest information) and authentication (password), it is possible to protect the document from being tampered with and to authenticate the

writer of the document simultaneously.

In the embodiment, the steps S13 and S14 in FIG.5 correspond to the signature generating part in claim 1 and the steps S15 and S16 in FIG.5  $\,$ 

5 correspond to the signature build-in part in claim 1.

Also, the step S43 in FIG.7 corresponds to the signature extracting part in claim 3 and the step S44 in FIG.7 corresponds to the digest obtaining part in claim 3.

The present invention is not limited to the specifically disclosed embodiments, variations and modifications, and other variations and modifications may be made without departing from the scope of the present invention.

The present application is based on Japanese Priority Application No. 11-332984 filed on November 24, 1999, the entire contents of which are hereby incorporated by reference.

#### WHAT IS CLAIMED IS:

5

10

15

1. An apparatus for authenticating a digital signature, comprising:

a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and

an image embedding part embedding the image information created by said signature synthesizing part into an indicated position in the digital document.

20

2. The apparatus as claimed in claim 1,
wherein said signature synthesizing part comprises an
image information generating part generating pixel
data for the image information including the digital
signature,

wherein:

a palette, where first color information is defined for first index information and second color information is defined for other index information, is referred to;

the first index information is defined for

pixels used for the predetermined mark; and

each of the other index information, which

corresponds to each number of a number string forming

the digital signature, is defined for each of other pixels.

5

3. The apparatus as claimed in claim 2, wherein said image information generating part assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

15

10

4. An apparatus for authenticating a digital signature, comprising:

a signature extracting part extracting the digital signature from image information embedded into a digital document;

a digest obtaining part decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and

an authenticating part determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by said digest obtaining part and authenticating the digital signature based on a result of the determination.

25

30

5. The apparatus as claimed in claim 5, wherein said signature extracting part refers to a palette where first color information is defined for first index information and second color information is defined for other index information, and defines partial pixel data, formed by removing the first index information from pixel data forming the image information, as the digital signature, so as to generate the digital signature.

10

5

- 6. A method for authenticating a digital signature, comprising the steps of:
  - (a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;
  - (b) creating image information by synthesizing the digital signature and a predetermined mark; and
- (c) embedding the image information
  25 created in said step (b) into an indicated position in the digital document.

30

20

- 7. A method for authenticating a digital signature, comprising the steps of:
- (a) extracting the digital signature from image information embedded into a digital document;
- 35 (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital

document has been tampered with; and

(c) determining whether second digest information regenerated based on the digital document identically corresponds to the first digest information obtained by said step (b) and authenticating the digital signature based on a result of the determination.

10

15

20

- 8. A computer-readable recording medium having a program recorded therein for causing a computer to authenticate a digital signature, said program comprising the codes of:
- (a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;
- (b) creating image information by synthesizing the digital signature and a predetermined mark; and
- (c) embedding the image information
  25 created in said step (b) into an indicated position in the digital document.

30

- 9. The computer-readable recording medium as claimed in claim 8, wherein said code (b) includes a code of (d) generating pixel data for the image information including the digital signature,
- 35 wherein:

a palette, where first color information is defined for first index information and second

color information is defined for other index
information, is referred to;

the first index information is defined for pixels used for the predetermined mark; and

each of the other index information, which corresponds to each number of a number string forming the digital signature, is defined for each of other pixels.

10

5

10. The computer-readable recording medium as claimed in claim 9, wherein said code (d)
15 assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

20

30

- 11. A computer-readable recording medium
  25 having a program recorded therein for causing a
   computer to authenticate a digital signature, said
   program comprising the codes of:
  - (a) extracting the digital signature from image information embedded into a digital document;
  - (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and
- (c) determining whether second digest
  information regenerated based on the digital document
  identically corresponds to the first digest
  information obtained by said code (b) and

authenticating the digital signature based on a result of the determination.

5

10

15

medium as claimed in claim 11, wherein said signature extracting part refers to a palette where first color information is defined for first index information and second color information is defined for other index information, and defines partial pixel data, formed by removing the first index information from pixel data forming the image information, as the digital signature, so as to generate the digital signature.

### ABSTRACT OF THE DISCLOSURE

In an apparatus for authenticating a digital signature, a signature generating part encrypts a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generates a digital signature. A signature synthesizing part creates image information by synthesizing the digital signature and a predetermined mark. And an image embedding part embeds the image information created by said signature synthesizing part into an indicated position in the digital document.

FIG.1

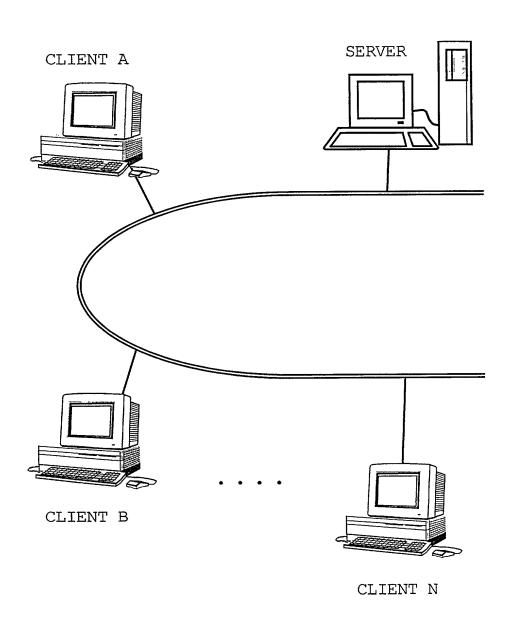


FIG.2

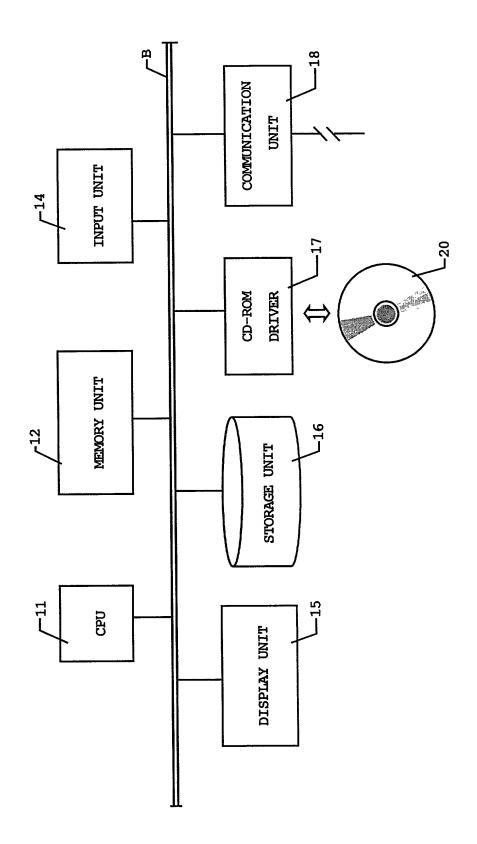
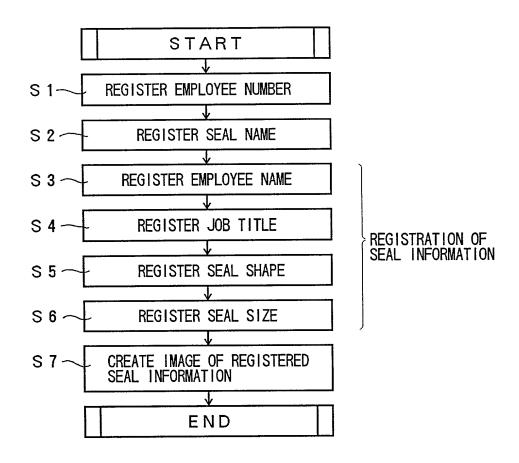


FIG. 3



# FIG. 4A

		<u>/</u> 41
SETTING OF SEAL-IMA	AGE PERSON INFORMATION	
EMPLOYEE NUMBER :	1 2 3 4 5 6 7 8 9 0	
SEAL NAME :		
REGISTER	CANCEL	

FIG. 4B

	43
REGISTRATION OF SEAL IMAGE	
NAME : FUJI JOB TITLE : DEVELOPM	ENT SECTION MANAGER
SEAL SHAPE: ROUND (DATE REQUIRED) \$\Bar{\psi}\$	DEVELOPMENT 4
SEAL SIZE : 1 2 mm	DEVELOPMENT SECTION MANAGER 03. 03. 98 FUJI
REGISTER CANCEL	

FIG. 5

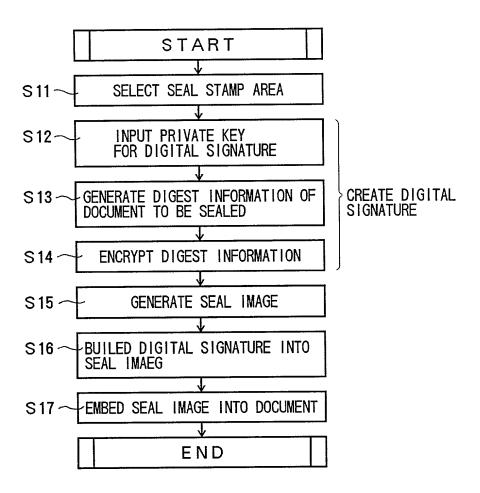


FIG. 6A

	61
	EXECUTION OF SEAL STAMP
	STAMP YOUR SEAL IN THE SELECTED AREA
	EMPLOYEE NUMBER: 1 2 3 4 5 6 7 8 9 0
STAMP	SEAL NAME :
63	PRIVATE KEY : *******
1	CONFIRM WHEN YOUR DOCUMENT IS DISPLAYED
	STAMP CANCEL

FIG. 6B

STAMP		CONFIRMATION OF STAMPED SEAL
DEVELOPMENT SECTION MANAGER 03. 03. 98 FUJI	67	STAMPED YOUR SEAL IN THE SELECTED AREA  OK  CANCEL

FIG. 7

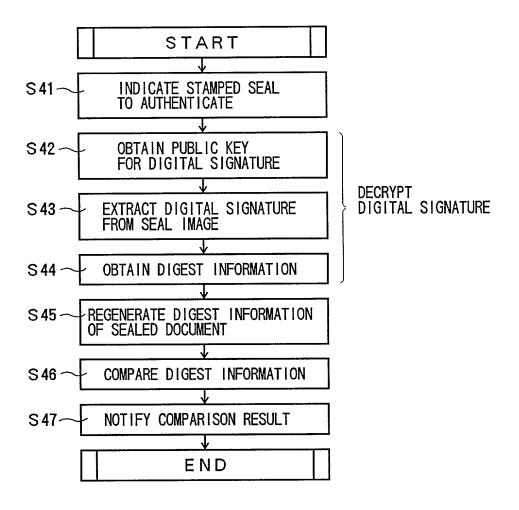


FIG. 8A

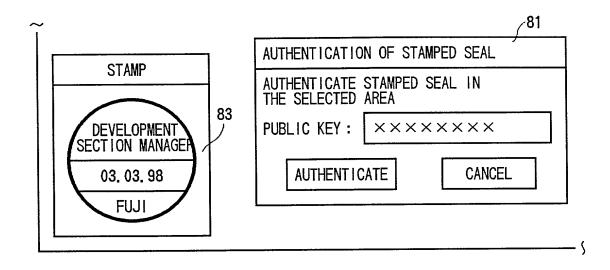


FIG. 8B

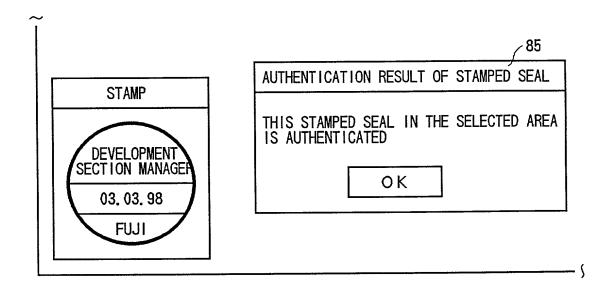
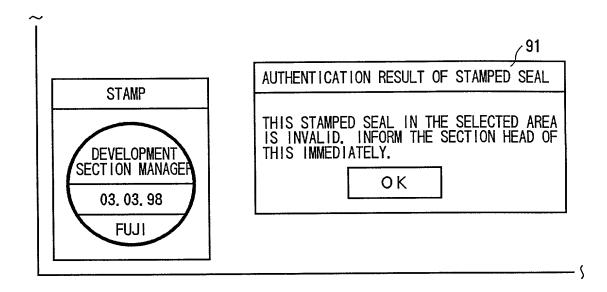
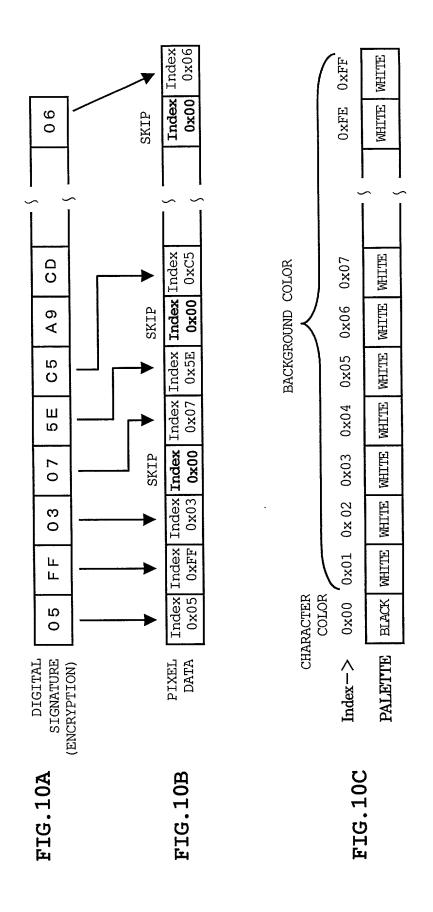


FIG. 9





# **Declaration and Power of Attorney For Patent Application**

特許出願宣言書及び委任状

#### Japanese Language Declaration

## 日本語宣言書

As a below named inventor, I hereby declar Phat:
My residence, post office address and citizenship are as stated next to my name.
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
APPARATUS AND METHOD FOR AUTHENTICATING
DIGITAL SIGNATURES AND COMPUTER-READABLE RECORDING MEDIUM THEREOF
the specification of which is attached hereto unless the following box is checked:  was filed on
I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.
l acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

# Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条 (a) - (d) 領文は365条 (b) 組に基金下記の、米 国以外の国の少なくとも一ヵ国を指定している特許協力条約 365 (a) 領に基ずく国際出顧、又は外国での特許出顧もしくは発明を確の出離についての外国優先権をここに主張するとともに、優先権を主張している。本出額の前に出顧された特許または発明者証の外国出顧を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

外国での先行出版 Pat. Appln. No.11-332984

L.

n

≆

į.

į.

AppIn。No.11-332984 Japan
(Number) (Country)
(肾号) (区名)

(Number) (Country)
(肾号) (河名)

記(、第35編米画法典119条(e)項に基いて下記の米 国特許出顧規定に記載された権利をここに主張いたします。

> (Application No.) (出顧書号)

(Filing Date) (出顧日)

私は、下記の米国法典第35編120条に基いて下記の米国
特許出順に記載された権利、又は米国を指定している特許 協力条約365条(c)に基ずく権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条 第1項又は特許協力条約で規定された方法で先行する米国特 許出顧に開示されていない限り、その先行米国出顧審提出日 以降で本出類書の日本国内または特許協力条約国際提出日ま での期間中に入手された、連邦規則法典第37編1条56項 で定義された特許資格の有無に関する重要な情報について開 示義務があることを認識しています。

(Application No.) (Filing Date) (出顧音号) (出顧日)

(Application No.) (Filing Date) (巴賴音号) (里賴日)

私は、私自身の知識に基ずいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じるところに基ずく芸明が全て真実であると信じていること、さらに故意になられた虚偽の表明及びそれと同等の行為は米国法典第18編第1001条に基ずき、罰金または有祭、もしくはその両方により処罰されること、そしてそのような故意による。成隣の声明を行なえば、出類した、又は既に許可された特許の行効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby claim foreign priority under Title 35, United States Code, Section 119 (a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Priority Not Claimed 優先権主要なし

24/November/1999 (Day/Month/Year Filed) (出版年月日)

(Day/Month/Year Filed) (出類年月日)

I hereby claim the benefit under Title 35. United States Code, Section 119(e) of any United States provisional application(s) listed below.

(Application No.)

(Filing Date)

(出類番号) (出類日)

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of application.

(Status: Patented, Pending, Abandoned) (現況: 特許許可濟、孫漢中、故養證)

(Status: Patented, Pending, Abandoned) (現況: 特許許可济、孫属中、放棄済)

knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the

I hereby declare that all statements made herein of my own

United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

# Japanese Language Declaration

(日本語宣言書)

委任状: 私は下記の発明者として、本出頭に関する一切の 手続きを米特許商標局に対して遂行する弁理上または代理人 として、下記の者を指名いたします。(弁護士、または代理 ^ 氏名及び登録番号を明記のこと)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application, and transact all business in the Patent and Trademark Office connected therewith (list name and registration number)

James D. Halsey, Jr., 22,729; Harry John Staas, 22,010; David M. Pitcher, 25,908; John C. Garvey, 28,607; J. Randall Beckers, 30,358; William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D. Stein, 37,240; Paul I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Marlette, 35,269; Harlan B. Williams, Jr., 34,756; George N. Stevens, 36,938; Michael C. Soldner, P-41,455 and William M. Schertler, 35,348 (agent)

普爾送付先

Send Correspondence to:

STAAS & HALSEY 700 Eleventh Street, N.W. Suite 500 Washington, D.C. 20001

直接電話連絡先: (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY (202) 434-1500

唯一または第一発明者	†名	Full name of sole or first inventor		
		Syuichi Satake		
発明者の署名	日付 .	Inventor's signature Symithi Satako 25, 2000		
住所		Residence		
		Nei, Japan		
<b>国籍</b>		Citzenship Japan		
私杏石		Post Office Address		
		c/o TOYAMA FUJITSU LIMITED,		
		2-1, Yasuuchi 2-chome, Yatsuo Machi,		
		Nei-Gun, Toyama, 939-2392 Japan		
第二共同発明者		Full name of second joint inventor, if an	у	
第二共同発明者	日付	Second inventor's signature	Date	
住所	<del></del>	Residence		
国籍		≟.⁄tizenship		
私書籍		Post Office Address		

(第三以降の共同発明者についても同様に記載し、署名をす ること)

(Supply similar information and signature for third and subsequent joint inventors.)